HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

MASTER THESIS

Herr
Grigory Devadze

Analysis of control system stability under algorithmic uncertainty

2016

Fakultät **Angewandte Computer- und Biowissenschaften**

MASTER THESIS

Analysis of control system stability under algorithmic uncertainty

Autor:
Grigory Devadze

Studiengang:
Applied Mathematics in Digital Media

Seminargruppe:
MA14w1

Erstprüfer:
Prof. Dr.-Ing. Alexander Lampe

Zweitprüfer:
Dr.-Ing. Pavel Osinenko

Mittweida, Dezember 2016

Bibliografische Angaben

Devadze, Grigory: Analysis of control system stability under algorithmic uncertainty, 29 Seiten, 5 Abbildungen, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften

Master Thesis, 2016

Referat

Stability of control systems is one of the central subjects in control theory. The classical asymptotic stability theorem states that the norm of the residual between the state trajectory and the equilibrium is zero in limit. Unfortunately, it does not in general allow computing a concrete rate of convergence particularly due to algorithmic uncertainty which is related to numerical imperfections of floating-point arithmetic. This work proposes to revisit the asymptotic stability theory with the aim of computation of convergence rates using constructive analysis which is a mathematical tool that realizes equivalence between certain theorems and computation algorithms. Consequently, it also offers a framework which allows controlling numerical imperfections in a coherent and formal way. The overall goal of the current study also matches with the trend of introducing formal verification tools into the control theory. Besides existing approaches, constructive analysis, suggested within this work, can also be considered for formal verification of control systems. A computational example is provided that demonstrates extraction of a convergence certificate for example dynamical systems.

I. Contents

II. List of Figures

III. Preface

Algorithmic uncertainty within the current work is understood as discrepancy between idealized mathematical algorithms and their numerical realizations. Algorithmic uncertainty may result, for example, from discretization and numerical approximation. In floating-point approximations, unexpected errors due to roundoff may occur. In contrast to the floating-point arithmetic, there exist so-called exact real number arithmetics, some of which use algorithmic representation of real numbers which potentially allow arbitrarily approximation of the given real number. Exact real number arithmetic is often used in automated theorem proving software [2–6]. An example of an automated and formalized proof is the proof of Kepler's conjecture [7]. The present thesis is focused on the issues of algorithmic uncertainty with regards to system stability.

System stability has been among the most crucial subjects of control theory. Traditionally, stability of control systems is analyzed within the Lyapunov theory [8] first introduced in 1892. The Lyapunov function method (also called second method of Lyapunov) lies in the heart of numerous controller designs found in literature. To certain extent, it generalizes the concept of mechanical energy to abstract systems. Dealing with the numerical uncertainty in connection with the proving of stability properties is a certain difficulty. Heuristics and post-processing are often required to quantify and to eliminate the uncertainties. Depending on the application's goal, numerical methods sometimes have to be adapted in order to fulfill requirements on the accuracy and robustness.

There is a relatively new but important framework, the so-called formal verification, that was suggested to address formal correctness of software and systems. Formal verification, i. e., verification of system's properties within some formal logical system, recently started attracting much attention of the control engineering community [9–16]. Formal correctness may be seen as a formal certificate ensuring that the behavior of the system matches with the designed one for the whole space of possible input conditions. As for the stability theory, it means providing a formal certificate, i. e., a certain mathematical construct, that assures boundedness or convergence of the system trajectories to the equilibrium. Incorrect functioning may drive the behavior away from the expected one. Consequences of failures may be as bad as damage to the devices and human health, not just deteriorated performance. In investigation of correctness of system's stability, one may be interested in answering the following questions: "What is a bound on the magnitude of a system trajectory starting from so or so initial condition?", "How fast does the trajectory converge to the equilibrium?". The classical Lyapunov theory does not in general provide answers to these questions. For example, finding an appropriate Lyapunov function candidate and showing negative definiteness of its time derivative ensures "energy decay" in the system and, consequently, convergence. However, the theory in general does not provide a rate of convergence. Even though it shows that the

limit of the metric between the system trajectory and the equilibrium is zero as time goes to infinity, it does not say how fast the said metric decays. It is so due to the classical definition of a limit. The definition merely states what the “value at infinity” is, but does not provide any information on the rate of convergence. To deal with this problem, the concept of exponential stability is sometimes used instead, but it is harder to verify than asymptotic stability. Perhaps, using a different notion of a limit, which would necessarily “encode” a rate of convergence and address algorithmic uncertainty, might provide a practically useful framework for formal verification of control system stability. This is the central question of the current study. In other words, what is necessary information to be provided within a Lyapunov function that allows “computing” the rate of convergence of the state trajectories up to any given precision thus having algorithmic uncertainty under control?

1 Introduction

1.1 Problem Statement

The current work proposes to revisit the control system stability theory with the aim of convergence rates under algorithmic uncertainty. The key ingredient of the proposal is the constructive analysis which is a mathematical tool that realizes equivalence between certain theorems and computation algorithms. The classical asymptotic stability theorem merely states that the norm of the residual between the state trajectory and the equilibrium is zero in limit. It does not in general allow computing the concrete rate of convergence. The stability theorem is revisited constructively which allows computing the convergence rates, also called convergence certificates in the current framework. The result requires, however, certain additional conditions on the Lyapunov function. Nevertheless, these conditions can be met in practice without a large extra design effort. The overall goal of the current study matches with the trend for introducing formal verification tools into the control theory. It is suggested that the constructive analysis might serve as one of the good starting points to this end. The computational example is provided that demonstrates extraction of a convergence certificate for a sample dynamical system. A formal stability certificate is, within the current study, a function of time, which may in general depend on the initial condition, which puts an upper bound on the metric between the system trajectory and the equilibrium.

The current work starts with a review of selected existing approaches to formal verification of control systems in Section 1.2 followed by a brief description of mathematical frameworks which may help address the stated problem (Section 2). In particular, a brief history and selected notions of constructive analysis, which is in the focus of the current work, are presented, in Section 2.1. A brief review of Lyapunov stability theory is given in Section 2.2. Section 2.3 is concerned with analysis of asymptotic stability with the goal of computing formal certificates of asymptotic stability whereas Section 2.4 presents a concrete algorithmic realization. Section 2.5 presents case studies.

1.2 Selected approaches to formal verification of control systems

Formal verification methods have been attracting attention of the control engineering community in the recent years and the proposed approaches are diverse. To demonstrate this, some selected ones are briefly reviewed in this section. They can be tracked to as early as the work of Livadas [17] where he addressed formal verification for collision avoidance in hybrid systems. The major apparatus used was hybrid input-output automata. The work suggested a special abstract notion – called protector – to guarantee compliance with safety requirement. Correctness proof of the protector was established within the theory of hybrid input-output automata. Similar issues were addressed by Franzle [18] where he investigated formal logics of hybrid automata and the related reachability issues. Later, Mysore et al. [19] applied formal logic of hybrid automata to systems biology. An important property of these two formal logic approaches was quantifier elimination, i. e., deriving formally true quantifier-free logical formulas.

In their project dedicated to formal verification methods to the European Train Control System (ETCS), Platzer et al. [20] also suggested to use quantifier elimination. The background formal system was differential dynamic logic.This is a first-order system for formalization of hybrid systems which can be generalized to formalize also differential equations. The ETCS was formalized and verified within the differential dynamic logic throughout an iterative process including the so-called controllability discovery, control refinement, safety convergence and liveness check steps. A more generalized and substantial description of the framework of differential dynamic logic applied to dynamical systems with an extensive set of examples was given in [9]. It is important to notice their background number field – the real closed field – that enables quantifier elimination [21]. Another firm application of differential dynamic logic can be found in Loos et al. [22] where they addressed safety of distributed aircraft systems. The works by Platzer et al. also offer a good literature review on the subject matter for an interested reader. Hybrid Hoare logic was used by Zou et al. [23] to formally verify a control system within the Chinese train network. They claimed to better address parallelism and communication issues within their approach than the one based on differential dynamic logic.

Automated theorem proving – performed by special software called proof assistants – also plays an important role in formal verification of control systems. For instance, Platzer et al. [24] developed automated theorem proving methods within their differential dynamic logic. Description of their software tool – KeYmaera – cay be found in [25]. Zou et al. [23] used Isabelle for implementation of their control system formal verification based on Hybrid Hoare logic. A tool called Why3 coupled with MATLAB/Simulink was used in more recent works by Araiza et al. [10, 26] to perform simple stability checks of linear discrete systems with quadratic Lyapunov functions. Their

method may be considered complimentary to the available model verifiers available within MATLAB/Simulink. [13] mentioned several automated theorem proving software tools to be considered for implementation of formal verification of control systems – Coq, HOL Light, Isabelle, Lean. His work also indicated the importance of the question raised within the current study. He suggested to address formal analysis of the theories like stability, including Lyapunov theory, observability, controllability, optimal, robust, and adaptive control. As a logical frameworks for computations, he suggested to use the Type Two Theory of Effectivity developed by Weihrauch (see, for example, [27–29]). This theory will be briefly reviewed in Section 2. Gao [13] also reviewed a solver called dReal for solving logical formulas in nonlinear dynamical systems theory. Siddique et al. [15] used HOL Light in their formalization of photonic systems. Among other aspects, they formalized difference equations and z-transform within the proof assistant. A recent work by Bernardeschi et al. [30] proposed to use the Prototype Verification System as the proof assistant for verification of a water level controller. Formalization of the behavior and safety requirement verification were carried out. The Munich project on formal verification of cyber-physical systems is another representative example. Within it, Althoff et al. [11, 12] extensively used reachability analysis with zonotopes for verification of power system stability and automated road vehicles respectively. Kong et al. [14] investigated applications of reachable sets to semi-algebraic dynamical systems with polynomial approximators of sets in Euclidean space as their central concept. They focused on inductive invariants which are certain properties of dynamical systems that hold from the initial state throughout the system trajectories. Chan et al. [16] recently also addressed formal verification of cyber-physical systems using Coq proof assistant. In their work, they addressed formal verification within the Lyapunov stability theory.

An ongoing European research project on formal verification of stability of embedded control systems (see description under `cordis.europa.eu/project/rcn/ /187016_en.html`) is dedicated to algorithmic methods of correctness check and also demonstrates the importance of the questions raised within the current study.

To summarize, the given review clearly indicates that application of different formal methods has certain merits for control theory, especially regarding tackling algorithmic uncertainty. The software tools and logical foundations are diverse. However, a certain effort is required for a control systems engineer to start working with the mentioned techniques since they are loaded with background in pure logic that is not usually largely represented within engineering education. This also concerns the Weihrauch's computable analysis suggested as the major framework by Gao [13]. In the next section, a brief description of computable analysis is provided. On the other hand, the next section also proposes another background mathematical foundation for formal analysis of control systems under algorithmic uncertainty – constructive analysis – and it will be shown such an approach might have a certain merit. It is believed that constructive analysis might better match with the mathematical education a control engineer usually receives. The details are given in the second part of the next section.

2 Mathematical frameworks for formal stability analysis

As was seen in the previous section, mathematical frameworks and logical systems for formal verification of control systems are diverse. Some of them, such as differential dynamic logic, might require certain background in formal logic to start using this approach. In this section, however, the focus is set on the Weihrauch's computable analysis and constructive analysis as developed by Bishop [31]. The Weihrauch's computable analysis has a notion of a computable mathematical object as the central concept. "Computable" in this context means effectively computable. That is, an algorithm computing the mathematical object in question must consist only of finitely many exact instructions, it needs to always terminate and produce a correct answer. The Weihrauch's computable analysis formalizes this concept and defines precisely what computable numbers, computable functions and other computable objects are. It relies on the notion of a Turing machine – an abstract device performs certain actions on a strip of tape – first formalized by Turing [32]. The real numbers are represented as infinite binary sequences produced by Turing machines. A function on real numbers is in turn called computable whenever there is a Turing machine which computes each infinite binary sequence representing a real number into some sequence representing the value of the function.

Roughly speaking, the Weihrauch's computable analysis mostly works with the said representations and shows that so or so mapping is computable. Even though, such a framework attracted some attention in the control engineering community, two subtleties need to be indicated. First, the background logic of the Type Two Theory of Effectivity is classical. Without going into detail so far, it means the following: the computations merely need to terminate, but there is no way to calculate the bound on the maximum number of iterations after which the computation finishes. This idea can be illustrated on the example of BlooP and FlooP programming languages introduced by Hofstadter [33] to illustrate certain logical derivations. Essentially, BlooP is a simple programming languages that allows only bounded loops – the "for ... do" loop. On contrary, FlooP allows unbounded loops such as "while ... do" loops. Unlike FlooP, BlooP is not Turing-complete in that one cannot program every computable function in it.

Another subtlety is the framework of the Weihrauch's computable analysis itself which is heavily formal and might be unusual for an engineer. Instead of numbers and functions, there are representations and Turing machines. Perhaps, it may be appropriate for certain formal verification problems, but the current study is concerned with mathematical framework for adressing algorithmic uncertainty and formal analysis – constructive analysis – which is briefly described further.

2.1 Brief overview of constructive analysis and selected notions

The history of constructive analysis began in 1907. The Dutch mathematician Brouwer criticized in his doctoral thesis several concepts of classical mathematics (further denoted by CLASS) and suggested the so-called intuitionistic mathematics (INT) as an alternative [34].

One of its interpretations is due to Brouwer, Heyting and Kolmogorov (sometimes called BHK interpretation or realizability interpretation) which states the fundamental logical rules for what can be interpreted as a mathematical proof [35]. Let P and Q be some arbitrary formulas. One of the most important rules in BHK are:

1. Proving the implication $P \Rightarrow Q$ means finding an algorithm that transforms a proof of P into a proof of Q
2. To prove $\exists a.P[a]$, an algorithm computing a and the proof that $P[a]$ holds are required.
3. To prove $\forall a \in A.P[a]$, an algorithm is required that converts $a \in A$ into a proof of $P[a]$.

One of the key difference to CLASS is: to prove $\exists a.P[a]$ classically, it suffices to show that $\neg\forall\neg P[x]$ whereas in INT such a proof is not allowed in general. In other words, impossibility of nonexistence is not equivalent to existence in general.

In 1948-1949 A. A. Markov introduced the so-called Russian school of constructive mathematics (RUSS) based on the Church-Markov-Thesis that states that all computable functions from the natural numbers to the natural numbers are computable . The logical principles of RUSS are widespread in complexity theory of computer science and its applications [36].

In 1967, E. Bishop published a monograph called "Foundations of Constructive Analysis" [37] where he revisited INT and developed a new kind of constructive mathematics that will be denoted by BISH here. BISH has the property that every proof in BISH is a valid proof in CLASS, INT and RUSS. Fig. 2.1 illustrates schematically this fact.

BISH can be described as mathematics with intuitionistic logical background along with certain set-theoretical principles. Keeping the intuitionistic logical background and making sure that the set-theoretic principles would not imply non-constructive claims lead to a framework in which every proof could be interpreted as an algorithm. The goal of Bishop [37] was to develop an analysis that would, on one hand, implement the constructive logic and be less formal so that anyone could use it without a strong background in logic just like most of the engineers tacitly work in the classical set theory, but

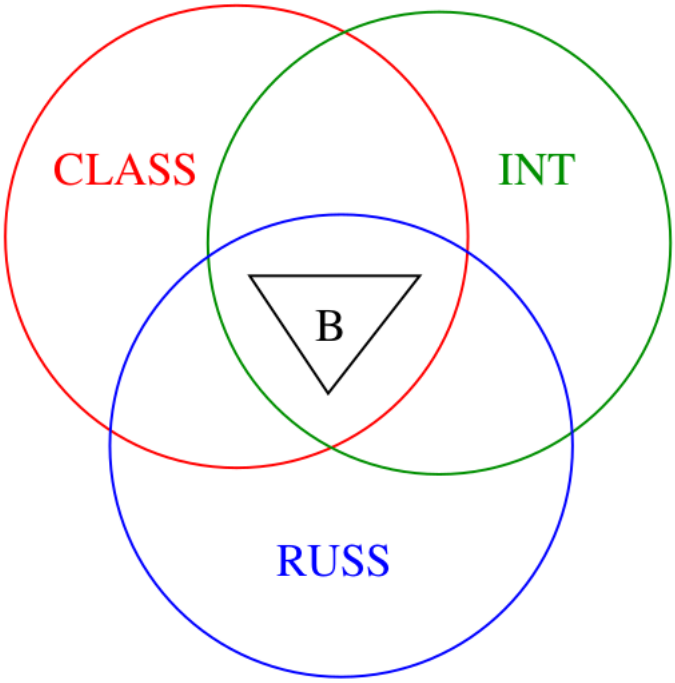

Figure 2.1: Consistency of BISH with CLASS, INT and RUSS. [1]

almost never refer to its axioms. This is not to say that constructive analysis does not have solid formal foundations. Interested reader may refer, for example, to Ye [38] for a rigorous derivation which is beyond the scope of the current work.

The central notion in Bishop's constructive analysis is an operation – a finite algorithm that produces a unique result in a finite number of steps for each input in its domain in a predictable way. The "predictable way" means a method of calculating the upper bound on iterations needed to get the result and control algorithmic uncertainty. This may be considered as one of the key differences between the Weihrauch's computable and Bishop's constructive analyses. For example, the above mentioned BlooP programming language can implement any said operation, but FlooP allows also programs that cannot be considered as operations. Perhaps, the best demonstration of these ideas is the constructive notion of a real number.

Definition 2.1 A real number x is a operation that calculates consecutive rational approximations to the real number with a predefined rate of convergence. In other words, a real number is regular Cauchy sequence of rational numbers in the sense that

$$\forall n, m \in \mathbb{N}. |x(n) - x(m)| \leq \frac{1}{n} + \frac{1}{m}.$$

Here, x is regarded as an operation and $x(n)$ means the nth rational approximation. As can be seen from the definition, the rate of convergence is controlled by the indices

n and m themselves. Equality of two arbitrary real numbers is in general undecidable since there is no algorithm that can decide whether $x = y$ or $x \neq y$ for $x, y \in \mathbb{R}$. Such an algorithm would be equivalent to solving the problem of deciding whether an arbitrary computer program terminates or not – which is impossible as shown by Turing [32].To say, for example, that $x < y$ means providing a witness or a certificate, a natural number n^* such that:

$$x(n^*) < y(n^*) - \frac{1}{n^*}.$$

Further, a set is a pair of operations: $\in$ determines that a given object is a member of the set, and $=$ determines whenever two given set members are equal. Such a technique is common in constructive analysis – every statement comes together with a certificate that verifies it. In turn, a proof means constructing a certificate. Treatment of logical formulas is performed in this spirit.

For example, proving a formula $\exists x \in A.\varphi[x]$ means deriving an operation that constructs an instance x along with a proof that $x \in A$ and a proof of the logical formula $\varphi[x]$. This operation with the said proof is called a certificate of $\exists x \in A.\varphi[x]$. Proving a formula $\forall x \in A.\varphi[x]$ means proving a quantifier-free formula $\varphi[x]$ with x being a free variable provided with a certificate for $x \in A$. Working in constructive analysis is somewhat similar to programming which may be seen more appropriate for a certain group of control system engineers than working in heavily abstract formal systems. On the other hand, any proof of a theorem in constructive analysis is (or can be made to) an algorithm whose correctness proof is the proof of the theorem itself. As an important consequence of constructive interpretation of analysis, the rule of excluded middle and in turn proof by contradiction is generally rejected.

The notion of a real number can generalized to the notion of a point in Euclidean space $\mathbb{R}^n$ in a straightforward manner. Euclidean space $\mathbb{R}^n$ is a normed space with the norm $\|x\| \triangleq \left(\sum_{i=1}^{n} (x_i)^2\right)^{\frac{1}{2}}$ where x_i is the ith coordinate of x.The metric is defined as $\|x - y\|$ for any $x, y \in \mathbb{R}^n$.

Particular attention is paid to those sets in Euclidean space which are called totally bounded:

Definition 2.2 A set $X \subset \mathbb{R}^n$ is called totally bounded if there is an operation that for any given positive rational number ε constructs a finite set $\{x_i\}_{i=1}^{N}$ of distinct points in X such that any $x \in X$ lies within an ε-ball centered at some x_i.

An important property of totally bounded sets of the real number line is that their infima and suprema exist constructively. Another important notion in constructive analysis is the notion of a function:

Definition 2.3 A function $f : \mathbb{R}^n \to \mathbb{R}^m$ is a pair of operations: one operation computes

rational approximations to $f(x)$ from rational approximations to $x \in \mathbb{R}^n$, and the second one, $\omega : \mathbb{Q}_{>0} \times \mathbb{Q}^n \times \mathbb{Q}_{>0} \to \mathbb{Q}$, called *modulus of continuity*, satisfies the formula:

$$\forall \varepsilon \in \mathbb{Q}_{>0}, c \in \mathbb{Q}^n, r \in \mathbb{Q}_{>0}, \forall x, y \in \{z : \|z-c\| \leq r\}$$
$$\|x-y\| \leq \omega(\varepsilon, c, r) \implies \|f(x)-f(y)\| \leq \varepsilon.$$

A modulus of continuity is an important certificate that every function in constructive analysis must have inside itself which allows computing bounds on the change of the argument that leads to a change of the function values within a prescribed bound. Functions can also be defined on general locally compact metric spaces, i. e., metric spaces whose bounded subsets are contained in compact subsets [31]. Let $C(X, \mathbb{R}^m)$ denote set of uniformly continuous functions from a totally bounded set $X \subset \mathbb{R}^n$ to $\mathbb{R}^m$.

In Section 2.3, a constructive analog of a particular Lyapunov stability theorem is addressed. It will use an important notion of a strictly increasing function (in norm). In constructive analysis, it is defined as follows:

Definition 2.4 A function $f : X \to \mathbb{R}$, where $X \subset \mathbb{R}^n$ is strictly increasing (in norm) if there is an operation $\nu : \mathbb{Q}^n \times \mathbb{Q}^n \to \mathbb{Q}_{>0}$ such that:

$$\forall x, y \in \mathbb{Q}^n . \|x\| < \|y\| \implies f(y) - f(x) > \nu(x, y).$$

This operation ν is called modulus of increase and certifies the statement "f is strictly increasing". This is another example of certifying statements in constructive analysis.

The following lemma is due to Bishop and Bridges [31] and allows computation of infima and suprema which are crucial in Section 2.3.

Lemma 2.5 *If $f : X \to \mathbb{R}$ is uniformly continuous and X is totally bounded, then* $\sup f$ *and* $\inf f$ *exist.*

Proof: Let ω_f be a modulus of continuity for f. For each $\varepsilon > 0$ let $x_1, ..., x_n$ be an $\omega_f(\varepsilon)$ approximation to X. Then for any point $x \in X$, there exists $i \in 1, ..., n$ such that $\|x - x_i\| \leq \omega_f(\varepsilon)$. It follows that the set $\{f(x_1), ..., f(x_n)\}$ is finite and an ε-approximation to $f(X)$. Thus the $\sup f$ and $\inf f$ exist. □

The next theorem is the approximate version of the intermediate value theorem and important corollary of this theorem is that if the function f possesses a certificate of being strictly increasing, then the inverse f^{-1} exists constructively. The calculation of inverse functions will be used later in Section 2.3.

Theorem 2.6 (Ye, [38]) *If $f \in C([a,b],\mathbb{R})$ and $f(a) < f(b)$, then for any y such that $f(a) \leq y \leq f(b)$, and for any $\varepsilon > 0$, there exists $x \in [a,b]$ such that $|f(x) - y| < \varepsilon$. Moreover if f is strictly increasing, then there exists $x \in [a,b]$ such that $f(x) = y$.*

Proof: Assume that $\varepsilon > 0$ is a rational number. Divide $[a,b]$ into small intervals $p_0 = a, ..., p_N = b$ such that $p_1, ..., p_{N-1}$ are rational numbers and $p_{i+1} - p_i \leq \omega_f(\varepsilon/7)$, where ω_f is a modulus of continuity for f. Therefore, $|f(p_{i+1} - f(p_i))| \leq \varepsilon/6$. For each p_i, we can choose a rational number q_i such that $|f(p_i) - q_i| < \varepsilon/6$ and let q be a rational such that $|y - q| < \varepsilon/6$. Then , $|q_{i+1} - q_i| < \varepsilon/2$. Since $f(a) \leq y \leq f(b)$, we have $q_0 - \varepsilon/3 \leq q \leq q_N + \varepsilon/3$. By comparing q with $q_0, ..., q_N$, we can find q_k such that $|q_k - q| < \varepsilon/2$. Since $|f(p_k) - q_k| < \varepsilon/6$ and $|y - q| < \varepsilon/6$, we have $|f(p_k) - y| < \varepsilon$.For the second half, note that f being strictly increasing implies that we have a term τ so that for rational number $p, q \in [a,b]$, if $p < q$, then $t(p,q)$ is a positive rational number such that $f(q) - f(p) > t(p,q)$. That is, $t(p,q)$ certificates that $f(p) < f(q)$ for $q > p$. Then to estimate x such that $f(x) = y$ up to the precision ε, we can divide $[a,b]$ into small rational intervals each of length $< \varepsilon/2$, and then for each interval $[p_i, p_{i+1}]$, we can approach y up to the precision of $t(p_i, p_{i+1})/2$ to decide if $f(p_i) < y$ or $y < f(p_{i+1})$. The estimate of x will be p_{i+1} with p_i the last one such that $f(p_i) < y$. □

Corollary 1 *If $f \in C([a,b],\mathbb{R})$ and f is strictly increasing, then there exists the inverse function $g \in C([f(a), f(b)],\mathbb{R})$, such that $f(g(y)) = y$ for $y \in [f(a), f(b)]$ and $g(f(x)) = x$ for $x \in [a,b]$.*

The next lemma allows extending functions on rational numbers to function of real numbers. It will be used in Section 2.3.

Lemma 2.7 (Extension Lemma, Bishop and Bridges, [31]) *Let Y be a dense subset of a metric space X, and $f : Y \to Z$ a uniformly continuous function from Y to a complete metric space Z, with modulus of continuity ω_f. Then there exists a uniformly continuous function $g : X \to Z$ with modulus of continuity $\frac{1}{2}\omega_f$ such that $f(y) = g(y)$ for all $y \in Y$.*

The next theorem is due to Ye [38] and adresses the initial value problems for the first-order ordinary differential equations which will also be used in Section 2.3 .

First, let $a, b > 0$, $(t_0, x_0) \in \mathbb{R}^2$,

$$D = [t_0 - a, t_0 + a] \times [x_0 - b, x_0 + b] \subset \mathbb{R}^2, \tag{2.1}$$

Let $f \in C(D,\mathbb{R})$. The goal is to find a function $\chi(t)$ such that χ is differentiable on an interval $I = [t_0 - c, t_0 + c], c \leq a$, and $(t, \chi(t)) \in D$ for $t \in I$ and

$$\chi(t_0) = x_0, \dot{\chi} = f(t, \chi(t)) \tag{2.2}$$

for $x \in I$. Such a function is called a solution of the initial value problem $x(t_0) = x_0, \dot{x} = f(t, x(t))$. Function $f(t,x)$ is called to satisfy the Lipschitz condition for x on D, if there exists L such that

$$|f(t,x_1) - f(t,x_2)| \leq L|x_1 - x_2| \tag{2.3}$$

Theorem 2.8 *Suppose that $f(t,x)$ is continuous on the rectangle $D : |t - t_0| \leq a, |x - x_0| \leq b$, and suppose that $f(t,x)$ satisfies the Lipschitz condition for x on the rectangle. Let $M = \max\{f(t,x) : (x,t) \in D\}$ and $\alpha = \min(a, b/M)$. Then, there exists a unique function χ differentiable on an interval $I = [t_0 - \alpha, t_0 + \alpha]$, such that $\chi(t_0) = x_0$ and $\chi_0(x) = \chi(t, \chi(t))$ for $t \in I$. Moreover, χ depends on its initial value x_0 uniformly continuously.*

In the next section, a fragment of the Lyapunov stability theory relevant for the current study is briefly described.

2.2 Brief overview of Lyapunov stability theory

The following section describes briefly the Lyapunov stability theory relevant to the current study and is mainly based on Khalil, [39].

Consider the following dynamical system:

$$\dot{x} = f(x,t), x \in \mathbb{R}^n, t \in \mathbb{R}_{\geq 0}. \tag{2.4}$$

Assume that $x_e = 0$ is an equilibrium point of (2.4).

Definition 2.9 The equilibrium point $x = 0$ of (2.4) is ,

- stable if, for each $\varepsilon > 0$, there is $\delta = \delta(\varepsilon, t_0) > 0$ such that

$$\|x(t_0)\| < \delta \Rightarrow \|x(t)\| < \varepsilon, \forall t \geq t_0 \geq 0 \tag{2.5}$$

- uniformly stable if, for each $\varepsilon > 0$, there is $\delta = \delta(\varepsilon)$, independent of t_0, such that is satisfied.
- asymptotically stable if it is stable and there is $c = c(t_0) > 0$ such that $x(t) \to 0$ as $t \to \infty$ for all $\|x(t_0)\| \leq c$.
- uniformly asymptotically stable if it is uniformly stable and there is $c > 0$, independent of t_0, such that for all $\|x(t_0)\| < c, x(t) \to 0$ as $t \to \infty$.

In this study, attention is restricted to the concept of the uniform asymptotic stability. Stability properties of the equilibrium point may dependent in general on starting time t_0 (Khalil, [39]). For example, consider the following system:

$$\dot{x} = -\frac{x}{1+t} \tag{2.6}$$

which has the closed-form solution

$$x(t) = x(t_0)\frac{1+t_0}{1+t} \tag{2.7}$$

The solutions are bounded via the condition $\|x(t)\| \leq \|x(t_0)\|$. Here, the constant c depends on t_0. The concept of uniform stability with respect to the initial time makes c independent from the starting time and is in the focus of the current work.

The following theorem states the necessary conditions for the equilibrium of (2.4) to be asymptotically stable [39, p. 100]:

Theorem 2.10 *Let $X \subset \mathbb{R}^n$ contain the origin and $V : X \to \mathbb{R}_{\geq 0}$ be a continuously differentiable function such that $V(x) = 0 \Leftrightarrow x = 0$ and $\dot{V}(x) < 0, x \in X \setminus \{0\}$. Then, $x_e = 0$*

is asymptotically stable.

Proof: (*Sketch*) The theorem implies that $x_e = 0$ is stable in the sense that for any ε there exists a δ such that $\|x(0)\| \leq \delta$ implies $\|x(t)\| \leq \varepsilon$ for all $t \geq 0$. Fix an $r \leq \varepsilon$. It suffices to show that for every χ, there exists τ such that $\|x(t)\| \leq \chi$ for all $t \geq \tau$. Since $V(x(t))$ is strictly decreasing and bounded below by zero, it follows that

$$\lim_{t\to\infty} V(x(t)) = v.$$

The fact that $v = 0$ can be shown by contradiction. Suppose that $v > 0$. Since V is continuous, there exists a $d > 0$ such that the closed ball $\mathscr{B}_d = \{x : \|x\| \leq d\} \subset X$ is contained in the set $\{x : V(x) \leq v\}$. The condition $v > 0$ implies that the trajectory $x(t)$ lies outside the ball $\mathscr{B}_d$ for all $t \geq 0$. Define $\theta =_{def} -\sup_{d\leq\|x\|\leq r} \dot{V}(x)$. This assignment is well-defined since the set $\{x : d \leq \|x\| \leq r\}$ is compact and $\dot{V}$ is continuous. But

$$V(x(t)) = V(x(0)) + \int_0^t \dot{V}(x(\tau))d\tau \leq V(x(0)) - \theta \cdot t.$$

The right-hand side must eventually become negative which contradicts the assumption that $v > 0$. □

As was mentioned in Section 2, proof by contradiction is in general forbidden in constructive analysis. The consequence for Theorem 2.10 is that although the limit of the norm of the system trajectory is zero, there is no computable way to predict the rate of convergence. In fact, the very notion of a limit in classical analysis does not require a computable rate of convergence. In the proof of the theorem, one might notice that for every χ, there exists a time τ after which the norm of the trajectory lies within χ, but there is unfortunately no way to actually calculate this τ. This is a usual consequence of proof by contradiction: some object is claimed to exist, but no concrete way of computing it is given. In contrast to this, every claim in constructive analysis comes with a certificate. As for Definition 2.9, to say that $\lim_{t\to\infty} \|x(t)\| = 0$ means providing a certificate that allows computing a rate of convergence. Such a certificate may be a positive-definite strictly decreasing function defined in a way analogous to that in Definition 2.4. This function then should serve as an upper bound on the norm of the system trajectory.

In the next section, the Lyapunov asymptotic stability theorem is revisited constructively.

2.3 Constructive stability analysis

In this section, the Lyapunov asymptotic stability theorem is addressed from the standpoint of constructive analysis as per Section 2. The goal is to obtain a constructive counterpart that would allow computation of the convergence certificates described in the previous section. First some basics of theorem proving tactics in constructive analysis are described. Then, Proposition 2.3.1 is stated and proven constructively followed by a particular algorithmic realization.

Two basics tactics in developing constructive counterparts of classical theorems are possible in constructive analysis. Sometimes, but rarely, the theorem can be proven constructively as it stands. But if not, there are two ways: one is to relax the claim of the theorem, e. g., prove an approximate version of the theorem, whereas the second is to strengthen the assumptions. In this section, the second way is chosen. As was discussed in Section 2, the classical Lyapunov stability theorem does not allow computing a convergence certificate. The goal of this section is to investigate the computational content of the stability theorem and to extract a particular algorithmic realization that calculates the rate of convergence of the system trajectories in norm. The following proposition is based on Theorem 3.8 of [39] and is the core of the current study:

Proposition 2.3.1 (See [40]) *Let X be the closed unit ball in $\mathbb{R}^n$ centered at the origin and $\dot{x} = f(x,t), x \in X$ be a dynamical system with the equilibrium point $x_e = 0$, such that $f(x,t)$ is Lipschitz-continuous in x. Suppose that there exists a continuously differentiable function $V : X \times [0,\infty) \to \mathbb{R}$ with the following properties:*

1. *There exists a strictly increasing function $w_1 : X \to \mathbb{R}$ such that*

$$\forall t \geq 0. \forall x \in X. w_1(x) \leq V(x,t)$$
$$w_1(0) = 0.$$

2. *There exists a function $w_2 : X \to \mathbb{R}, w_2(0) = 0$, a positive rational number ξ such that*

$$\forall \|x\| \geq \|y\|. w_2(x) - w_2(y) \geq \xi(\|x\| - \|y\|),$$

   and $\forall t \geq 0. \forall x \in X. V(x,t) \leq w_2(x)$.
3. *There exists a Lipschitz-continuous strictly increasing function $w_3 : X \to \mathbb{R}, w_3(0) = 0$ such that*

$$\forall t \geq 0. \forall x \in X. \dot{V}(x,t) \leq -w_3(x)$$

Then, $x_e = 0$ is asymptotically stable for any $x(0) \in X$.

Proof: Define the following functions:

$$\hat{\alpha}_1(s) =_{def} \inf_{s \leq \|x\| \leq 1} w_1(x)$$
$$\hat{\alpha}_2(s) =_{def} \sup_{\|x\| \leq s} w_2(x)$$
$$\hat{\alpha}_3(s) =_{def} \inf_{s \leq \|x\| \leq 1} w_3(x)$$

for any rational $s \in [0,1]$. First, observe that a sphere $\mathscr{S}_r =_{def} \{x : \|x\| = r\}, r \in \mathbb{Q}$ is a totally bounded set since a sequence of points with pure rational coordinates on $\mathscr{S}$ can be constructed that ε-approximates any point on $\mathscr{S}$ for any given ε. Consequently, the set $A =_{def} \{x : s \leq \|x\| \leq r\} \subset \mathbb{R}^n, s, r \in \mathbb{Q}$ is also totally bounded. The certificate of total boundedness can be constructed by appropriately choosing radii of concentric spheres and approximating each one including $\mathscr{S}_s$ and $\mathscr{S}_r$. Since the functions w_1, w_2 and w_3 are continuous, the functions $\hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3$ are constructively well-defined by Lemma 2.5. By Lemma 2.7 , $\hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3$ can be extended to the entire unit interval. Denote the extensions by $\alpha_1, \alpha_2, \alpha_3$ respectively. By Theorem 2.6, it follows that the inverse function α_2^{-1} can be constructed since α_2 is a continuous strictly monotonic function on a compact set. Moreover, α_2^{-1} is strictly increasing and Lipschitz-continuous, since α_2 by construction satisfies the following condition:

$$\forall s \geq r. \alpha_2(s) - \alpha_2(r) \geq \xi(s - r)$$

To see this, observe that $s = \alpha_2^{-1}(s')$ and $r = \alpha_2^{-1}(r')$ for some s', r' in the respective domains. Then, the condition implies that

$$\alpha_2(\alpha_2^{-1}(s')) - \alpha_2(\alpha_2^{-1}(r')) \geq \xi(\alpha_2^{-1}(s') - \alpha_2^{-1}(r'))$$

which yields

$$(\alpha_2^{-1}(s') - \alpha_2^{-1}(r')) \leq \frac{1}{\xi}(s' - r').$$

The following conditions evidently hold:

$$\alpha_1(\|x\|) \leq V(x,t) \leq \alpha_2(\|x\|),$$
$$\dot{V}(x,t) \leq \alpha_3(\|x\|)$$

for any $t \geq 0$ and $x \in X$. Further,by Theorem 2.8, since f is Lipschitz-continuous and X is compact, system trajectories starting from all $x_0 \in X$ exist. The next step is to show boundedness of the system trajectories. To this end, notice that since w_1 is strictly increasing, it follows that α_1 is a strictly increasing continuous function on a compact set and α_1^{-1} in turn exists and is also strictly increasing. It follows that $\alpha_1^{-1}(V_0) \geq \|x_0\|$.

The following condition holds:

$$\|x(t)\| \leq \alpha_1^{-1}(V(x(t),t))$$

for all $t \geq 0$ and any initial condition $x_0 \in X$. In particular, for any $x \in X$ and $t \geq 0$,

$$\alpha_1^{-1}(V(x,t)) \leq \alpha_1^{-1}(V(x,0)) \leq \alpha_1^{-1}\left(\sup_{x\in X} V(x,0)\right)$$
$$\implies \forall t \geq 0. \|x(t)\| \leq \alpha_1^{-1}\left(\sup_{x\in X} V(x,0)\right)$$

which verifies the boundedness of the system trajectories as required. Now consider the following differential inequality:

$$\dot{V} \leq -\alpha_3(\|x\|) \leq -\alpha_3(\alpha_2^{-1}(V))$$

Since α_2^{-1} and α_3 are Lipschitz-continuous, so is their composition. Therefore, there exists a function γ which is a unique solution of the initial value problem

$$\dot{y} = -\alpha_3(\alpha_2^{-1}(y)), \tag{2.8}$$
$$y_0 = V(x_0,0), \tag{2.9}$$

for some $x_0 \in X$ by Theorem 2.8. Moreover, the solution depends on the initial condition continuously. Denote the solution emitting from some y_0 by $\sigma(y_0,t)$. Then, it follows that

$$\dot{V} \leq -\alpha_3(\alpha_2^{-1}(V)) \Rightarrow \int_0^t \dot{V}\mathrm{d}\tau \leq -\int_0^t \alpha_3(\alpha_2^{-1}(V))\mathrm{d}\tau \Rightarrow$$
$$V - V(x_0,0) \leq \sigma(y_0,t) - y_0 \Rightarrow V \leq \sigma(y_0,t).$$

It can be shown that $\sigma(y_0,t)$ is a strictly decreasing function in t with the property that $\lim_{t\to\infty} \sigma(y_0,t) = 0$. To show that, define $\alpha^* =_{def} \alpha_3 \circ \alpha_2^{-1}$ and let $Y(y) =_{def} -\int_a^y \frac{1}{\alpha^*(z)}\mathrm{d}z$ for some $0 < a \leq y_0$ and any $0 < y \leq y_0$. Since α^* is strictly increasing, $\frac{1}{\alpha^*}$ is strictly decreasing and $-\frac{1}{\alpha^*}$ in turn is strictly decreasing. It follows that Y is strictly decreasing. Since Y is strictly decreasing and $Y(z) \geq 0$ for all $z \leq a$, it follows that $\sigma(y_0,t) \geq 0, \forall t \geq 0$. Furthermore, function Y has the property that

$$\lim_{y\to 0^+} Y(y) = \infty.$$

To see this, fix some $0 < \delta < \frac{a}{2}$. For any $0 < \varepsilon < \frac{a}{2}$, it follows that

$$\lim_{\varepsilon\to 0^+} \int_a^\varepsilon \frac{-1}{\alpha^*(z)}\mathrm{d}z = \lim_{\varepsilon\to 0^+}\left(\int_\varepsilon^{\varepsilon+\delta} \frac{1}{\alpha^*(z)}\mathrm{d}z + \int_{\varepsilon+\delta}^a \frac{1}{\alpha^*(z)}\mathrm{d}z\right)$$

$$\geq \lim_{\varepsilon \to 0^+} \left(\frac{\delta}{\alpha^*(\varepsilon+\delta)} + \int_{\varepsilon+\delta}^{a} \frac{1}{\alpha^*(z)} \right) = \infty$$

since $\alpha^*(0) = 0$. On any compact set $[\varepsilon, y_0], \varepsilon > 0$, Y^{-1} exists and for any $t \leq t^* =_{def} Y(\varepsilon) + Y(y_0)$ it follows that

$$\sigma(y_0, t) = Y^{-1}(Y(y_0) + t) \leq \varepsilon$$

due to the fact that

$$Y(\sigma(y_0, t)) - Y(y_0) = t$$

and because Y is strictly decreasing. For any $\varepsilon_1 > \varepsilon$, it follows that for all $t^* \leq t \leq t_1^* =_{def} Y(\varepsilon_1) + Y(y_0)$,

$$\sigma(y_0, t) < \sigma(y_0, t^*) \leq \varepsilon.$$

Therefore, for any $\varepsilon > 0$ there exists a t^* such that $\sigma(y_0, t) \leq \varepsilon$ for all $t \geq t^*$ which means

$$\lim_{t \to \infty} \sigma(y_0, t) = 0.$$

Since $\|x(t)\| \leq \alpha_1^{-1}(\sigma(y_0, t)) =_{def} \gamma(y_0, t)$ for all $t \geq 0$ and any initial condition $x_0 \in X$, it follows that $\lim_{t \to \infty} \|x(t)\| = 0$ for any x_0 in X. □

Proposition 2.3.1 can be seen as a possible constructive counterpart of Theorem 2.10 of Section 2.2. According to the requirement that an asymptotically stable equilibrium needs to possess a convergence certificate, the strictly decreasing function $\gamma(y_0, t)$ can be seen as a convergence certificate. It can be used to assess how fast the system trajectories decay to zero in norm. Setting $\sup_{x \in X} V(x, 0)$ as the initial condition in the problem (2.9), a particular certificate $\gamma(t)$ can be computed which indicates the "worst" bound on the norm of the system trajectories for the given functions w_1, w_2, w_3. Such a "worst" convergence certificate will be in the focus of the case study in Section 2.5.

2.4 Algorithmic realization

Further, Proposition 2.3.1 can be realized in the following simple algorithms. The first one, Algorithm 1, certifies the fact that the annuli $\{x : s \leq \|x\| r\}, s, r \in \mathbb{Q}$ used in the proof are totally bounded.

Algorithm 1 Construction of a total boundedness certificate for $\{x : s \leq \|x\| \leq r\} \subset \mathbb{R}^2, s, r \in \mathbb{Q}$

Require: $\varepsilon \in \mathbb{Q}$ and $s, r \in \mathbb{Q}, 0 \leq s \leq r \leq 1$
  Initialize $S =_{def} \emptyset$
  if $r = 0$ **then**
    Add point $(0,0)$ to S
  for $a \in \{s, s+\varepsilon, \ldots, r\}$ **do**
    $\theta_a =_{def} 2\arcsin(\frac{\varepsilon}{2a})$
    for $\theta \in \{0, \theta_a, 2\theta_a, \ldots, 2\pi\}$ **do**
      Add point $(a\cos(\theta), a\sin(\theta))$ to S
  return S

For demonstration purposes, the two-dimensional case is considered. For the case $x \in \mathbb{R}^n, n > 2$, this algorithm would require a modification, but it is beyond the scope of the current study. In Algorithm 1, $\sin, \cos, \arcsin$ need to be approximated sufficiently.
The second one, Algorithm 2, computes the function $\inf_{r \leq \|x\| \leq 1} f$ for a scalar-valued function f on the unit ball of $\mathbb{R}^2$.

Algorithm 2 Construction of $\inf_{r \leq \|x\| \leq 1} f$

Require: $\varepsilon \in \mathbb{Q}, r \in \mathbb{Q}, 0 \leq r \leq 1$ and a function f
  Set δ such that $\forall x, y. \|x - y\| \leq \delta \implies |f(x) - f(y)| \leq \varepsilon$
  Call Algorithm 1 with the parameters $(\delta, r, 1)$ and get a total boundedness certificate S
  return $\min_S f(S)$

An algorithm for computing $\sup_{0 \leq \|x\| \leq r} f, r \leq 1$ is analogous to Algorithm 2.

The next algorithm, Algorithm 3, computes the inverse of a strictly increasing function.

Algorithm 3 Construction of f^{-1} for a function $f : I \to \mathbb{R}$ where I is a non-trivial interval

Require: $\varepsilon, y \in \text{range}(f)$ and a function f

Set P to be a partition of I into subintervals of length less than $\frac{\varepsilon}{2}$

Decide for each subinterval $[p_i, p_{i+1}] \in P$ whether $f(p_i) < y$ or $y < f(p_{i+1})$

return p_{i+1} such that $f(p_i) < y$

In Algorithm 3, the second step is constructively valid since there is a modulus of increase within f that allows the case distinction $f(p_i) < y$ or $y < f(p_{i+1})$. Solutions of initial value problems can be computed by Picard iteration provided that the subject function satisfies the Lipschitz condition in the domain of interest [41]. Constructive proof of the Picard-Lindelöf theorem and details of the algorithm may be found in [38]. The current section was concerned with development of a constructive counterpart of Theorem 2.10 on asymptotic stability which resulted in Proposition 2.3.1. A particular algorithmic realization was provided. The next section demonstrates a particular application of these algorithms to investigating stability of a sample dynamical system.

2.5 Case study and discussion

Application of Proposition 2.3.1 is demonstrated for the following nonlinear dynamical system:

$$\begin{aligned}\dot{x}_1 &= -x_1 + x_1 \frac{e^{-x_1^2}}{1+x_1^2} - x_2 \tanh(t),\\ \dot{x}_2 &= -x_2 + x_2 \frac{e^{-t^2}}{1+x_2^2} + x_1 \tanh(t).\end{aligned} \tag{2.10}$$

It can be shown that $V(x,t) \equiv v\|x\|^2$ is a Lyapunov function for the system (2.10) for any positive number v. By setting

$$\begin{aligned}w_1(x) &:= v\|x\|^2,\\ w_2(x) &:= \begin{cases} v\chi\|x\|, \|x\| \leq \chi,\\ v\chi\|x\|^2, \|x\| \geq \chi \end{cases}\\ w_3(x) &:= 2v\left(\|x\|^2 - x_1^2\frac{e^{-x_1^2}}{1+x_1^2} - \frac{x_2^2}{1+x_2^2}\right),\end{aligned}$$

for any rational number $0 < \chi < 1$ the conditions of Proposition 2.3.1 are satisfied and the convergence certificate can be thus computed. In the current study, χ was set to 0.1. Fig. 2.2 illustrates the function w_3 for the case $v = \frac{1}{2}$ which is commonly used in stability analyses.

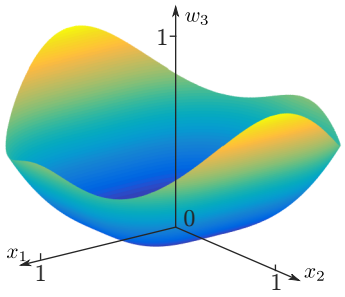

Figure 2.2: Function w_3 – upper bound on the derivative of the Lyapunov function

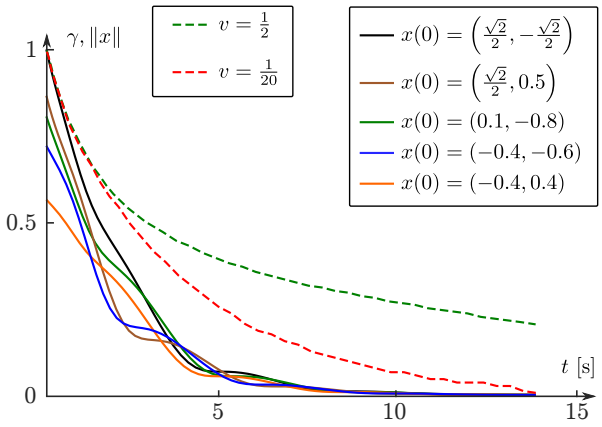

Figure 2.3: Convergence certificate and example system trajectories

The certificate γ as per Proposition 2.3.1 was computed. As can bee seen in Fig. 2.3, which illustrates the norm of several example system trajectories, the certificate for $v = \frac{1}{2}$ is relatively conservative. For testing purposes, another certificate – for $v = \frac{1}{20}$ – is illustrated as well.

Fig. 2.4 illustrates how the certificate for $v = \frac{1}{20}$ bounds some example system trajectories.

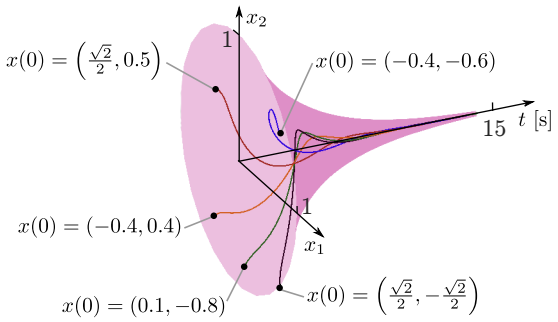

Figure 2.4: Three-dimensional illustration of the convergence certificate and example system trajectories

Finally, Fig. 2.5 shows the the level sets of the certificate.

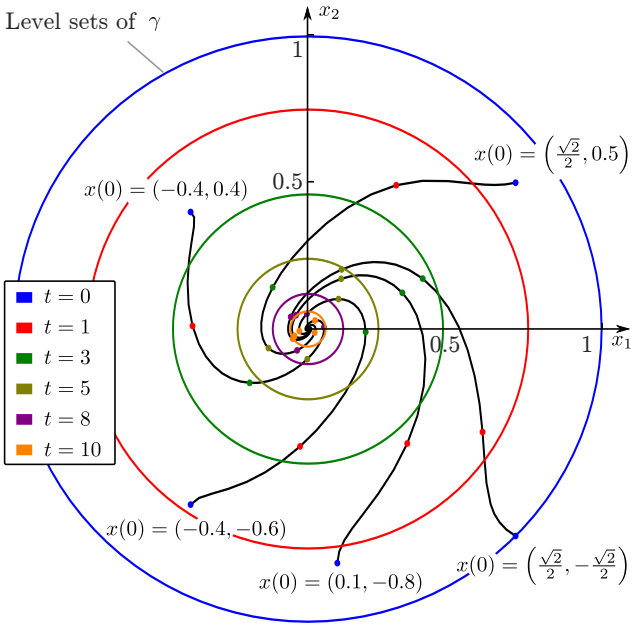

Figure 2.5: Levels sets of the convergence certificate and example system trajectories

It can be noticed that the second certificate is more tight. This fact demonstrates the idea that the convergence certificates as per Proposition 2.3.1 are properties of Lyapunov functions. That means: there may exist Lyapunov functions that provide better convergence certificates that others. Such an observation requires further investigation and might lead to development of a tool for assessment of different feedback controllers. This may be performed as follows: the designer builds a feedback controller and a Lyapunov function to prove stability of the closed-loop system. As per parametrization and structure of the controller, different convergence certificates may arise which may help compare and evaluate the controllers.

The proposed approach might be reminiscent of the so-called verified integration [42,43] where propagation of sets through dynamical systems is studied. However, the computation resulting from Proposition 2.3.1 is based on a formal proof of convergence whereas simulation of a dynamical system itself cannot serve as a proof of its stability. Furthermore, computation emerging from Proposition 2.3.1 requires solving a differential equation that does not explicitly depend on the system dynamics, but rather on certificates w_1, w_2 and w_3 of the Lyapunov function. Perhaps, constructive analysis of verified integration might provide more insight, but it is left as a possible future task.

3 Conclusion

This work suggested to formally study a fragment of the Lyapunov stability theory with the goal of addressing algorithmic uncertainty. As the foundation, constructive analysis was proposed. Unlike several existing formal approaches, constructive analysis is less loaded with abstract logical derivations and is closer to the usual classical analysis that a control systems engineer is familiar with. It is believed that such an approach may have its merit for control theory. It was indicated which parts of the classical asymptotic stability theorem did not provide computable results, and in contrast to it, a constructive counterpart was proven which was based on so called certificates. Algorithm extraction was demonstrated for calculating the convergence certificates. A case study showed results of computation convergence certificates for an example dynamical system.

Bibliography

[1] D. S. Bridges and I. Loeb. Glueing continuous functions constructively. *Archive for Mathematical Logic*, 49(5):603–616, 2010.

[2] O. Russell. Certified exact transcendental real number computation in coq. In *International Conference on Theorem Proving in Higher Order Logics*, pages 246–261. Springer, 2008.

[3] S. Boldo, C. Lelay, and G. Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, pages 1–38.

[4] L. Cruz-Filipe, H. Geuvers, and F. Wiedijk. C-corn, the constructive coq repository at nijmegen. In *International Conference on Mathematical Knowledge Management*, pages 88–103. Springer, 2004.

[5] B. Akbarpour and L. C. Paulson. Metitarski: An automatic theorem prover for real-valued special functions. *Journal of Automated Reasoning*, 44(3):175–205, 2010.

[6] N. Julien. *Certified Exact Real Arithmetic Using Co-induction in Arbitrary Integer Base*, pages 48–63. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[7] T. C. Hales, J. Harrison, S. McLaughlin, T. Nipkow, S. Obua, and R. Zumkeller. A revision of the proof of the kepler conjecture. In *The Kepler Conjecture*, pages 341–376. Springer, 2011.

[8] A. M. Lyapunov. The General Problem of the Stability of Motion (in Russian). *International Journal of Control*, 55(3):531–534, 1992.

[9] A. Platzer. Logics of dynamical systems. In *Proceedings of the 2012 27th Annual IEEE/ACM Symposium on Logic in Computer Science*, LICS'12, pages 13–24. IEEE Computer Society, 2012.

[10] D. Araiza-Illan, K. Eder, and A. Richards. Formal verification of control systems' properties with theorem proving. In *Control (CONTROL), 2014 UKACC International Conference on*, pages 244–249, 2014.

[11] M. Althoff and J. M. Dolan. Online verification of automated road vehicles using reachability analysis. *IEEE Transactions on Robotics*, 30(4):903–918, 2014.

[12] M. Althoff. Formal and compositional analysis of power systems using reachable sets. *IEEE Transactions on Power Systems*, 29(5), 2014.

[13] S. Gao. Descriptive control theory: A proposal. *arXiv preprint arXiv:1409.3560*, 2014.

[14] H. Kong, F. He, X. Song, M. Gu, H. Tan, and J. Sun. Safety verification of semi-algebraic dynamical systems via inductive invariant. *Tsinghua Science and Technology*, 19(2):211–222, 2014.

[15] U. Siddique, O. Hasan, and S. Tahar. Formal modeling and verification of integrated photonic systems. In *In Proceedings of the 9th Annual IEEE International Systems Conference (SysCon)*, pages 562–569, 2015.

[16] M. Chan, D. Ricketts, S. Lerner, and G. Malecha. Formal verification of stability properties of cyber-physical systems. 2016.

[17] C. Livadas. Formal verification of safety-critical hybrid systems. *Massachusetts Institute of Technology*, 1997.

[18] M. Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In *International Workshop on Computer Science Logic*, pages 126–139. Springer, 1999.

[19] V. Mysore, C. Piazza, and B. Mishra. Algorithmic algebraic model checking ii: Decidability of semi-algebraic model checking and its applications to systems biology. In *International Symposium on Automated Technology for Verification and Analysis*, pages 217–233. Springer, 2005.

[20] A. Platzer and J.-D. Quesel. European train control system: A case study in formal verification. In *International Conference on Formal Engineering Methods*, pages 246–265. Springer, 2009.

[21] A. Tarski. A decision method for elementary algebra and geometry. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 24–84. Springer, 1998.

[22] S. M. Loos, D. Renshaw, and A. Platzer. Formal verification of distributed aircraft controllers. In *Proceedings of the 16th international conference on Hybrid systems: computation and control*, pages 125–130. ACM, 2013.

[23] L. Zou, J. Lv, S. Wang, N. Zhan, T. Tang, L. Yuan, and Y. Liu. Verifying chinese train control system under a combined scenario by theorem proving. In *Working*

Conference on Verified Software: Theories, Tools, and Experiments, pages 262–280. Springer, 2013.

[24] A. Platzer. *Differential dynamic logics-automated theorem proving for hybrid systems*. PhD thesis, Universität Oldenburg, 2008.

[25] A. Platzer and J.-D. Quesel. Keymaera: A hybrid theorem prover for hybrid systems (system description). In *International Joint Conference on Automated Reasoning*, pages 171–178. Springer, 2008.

[26] D. Araiza-Illan, K. Eder, and A. Richards. Verification of control systems implemented in simulink with assertion checks and theorem proving: A case study. In *In Proceedings of the 2015 European Control Conference (ECC)*, pages 2670–2675. IEEE, 2015.

[27] K. Weihrauch. *Computability, EATCS Monographs in Theoretical Computer Science*. Springer Verlag, 1987.

[28] K. Weihrauch. A foundation for computable analysis. In *International Conference on Current Trends in Theory and Practice of Computer Science*, pages 104–121. Springer, 1997.

[29] K. Weihrauch. *Computable Analysis: an Introduction*. Springer Science & Business Media, 2012.

[30] C. Bernardeschi and A. Domenici. Verifying safety properties of a nonlinear control by interactive theorem proving with the prototype verification system. *Information Processing Letters*, 116(6):409–415, 2016.

[31] E. Bishop and D. Bridges. *Constructive analysis*, volume 279. Springer Science & Business Media, 1985.

[32] A. Turing. On computable numbers, with an application to the entscheidungsproblem. *J. of Math*, 58(345-363):5, 1936.

[33] D. Hofstadter. Gödel, Escher, Bach, 1975.

[34] L.E.J. Brouwer. *On the Foundations of Mathematics*. Ph.D. thesis, 1907.

[35] R.S. Buss. Handbook of proof theory. volume 137. Elsevier, 1998.

[36] A. S. Troelstra. History of constructivism in the 20th century.

[37] E. Bishop. *Foundations of constructive analysis*, volume 60. McGraw-Hill New York, 1967.

[38] F. Ye. *Strict finitism and the logic of mathematical applications.* Springer, 2011.

[39] H. Khalil. *Nonlinear Systems*. Prentice-Hall, 1996.

[40] P. Osinenko, G. Devadze, and S. Steif. Constructive analysis of control systems stability (submitted manuscript). In *In Proceedings of the 20th IFAC World Congress*, 2016.

[41] E. Coddington and N. Levinson. *Theory of Ordinary Differential Equations*. New York: McGraw-Hill, 1955.

[42] M. Berz and K. Makino. Verified integration of odes and flows using differential algebraic methods on high-order taylor models. *Reliable Computing*, 4(4):361–369, 1998.

[43] M. Berz, K. Makino, and J. Hoefkens. Verified integration of dynamics in the solar system. *Nonlinear Analysis: Theory, Methods & Applications*, 47(1):179–190, 2001.

Erklärung

Hiermit erkläre ich, dass ich meine Arbeit selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt und die Arbeit noch nicht anderweitig für Prüfungszwecke vorgelegt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Mittweida, 14. Dezember 2016